WHITEPAPER: USULAN PEMBENTUKAN ANGKATAN SIBER INDONESIA (ASI)

BAB 1: RINGKASAN EKSEKUTIF.....3

BAB 2: LATAR BELAKANG DAN URGENSI..... 4

2.1 Ancaman Cyber Warfare di Tingkat Global dan Nasional..... 4

2.2 Rentannya Pertahanan Siber Nasional: Studi Kasus di Indonesia.....5

2.3 Perkembangan Regulasi: Celah dalam Aspek Pertahanan Militer..... 5

2.4 Fragmentasi Kelembagaan: Tumpang Tindih dan Celah Koordinasi.....6

2.5 Pelajaran dari Komunitas Internasional..... 6

BAB 3: LANDASAN HUKUM DAN KEBIJAKAN.....7

3.1 Landasan Yuridis Nasional: Undang-Undang dan Peraturan Presiden.....7

3.2 Kepatuhan pada Hukum Internasional: Prinsip dalam Cyber Warfare..... 9

3.3 Perbandingan dan Praktik Terbaik (Best Practices) Internasional.....10

BAB 4: VISI, MISI, DAN FUNGSI..... 11

4.1 Visi..... 11

4.2 Misi..... 12

4.3 Fungsi Inti..... 13

BAB 5: STRUKTUR ORGANISASI DAN KOORDINASI.....14

5.1 Posisi dan Struktur Komando..... 14

5.2 Peran dan Tugas Tiap Unit.....16

5.3 Model Koordinasi Antar Lembaga.....17

BAB 6: SUMBER DAYA DAN SUMBER DAYA MANUSIA (SDM).....18

6.1 Kebutuhan SDM: Memburu Talenta Spesialis..... 19

6.2 Pendidikan dan Pelatihan: Membangun Pipa Regenerasi dari Hulu ke Hilir.20

6.3 Pola Rekrutmen dan Kerja Sama Internasional..... 21

BAB 7: KAPABILITAS TEKNIS DAN INFRASTRUKTUR.....22
7.1 Pilar Kapabilitas Teknis.....23
7.2 Penjaminan Keamanan Vital Information Infrastructure (VII).....25
7.3 Kolaborasi Riset dan Pengembangan (R&D).....25

BAB 8: PENDANAAN DAN ANGGARAN.....26
8.1 Estimasi Kebutuhan Anggaran.....27
8.2 Model dan Sumber Pembiayaan.....28

BAB 9: ROADMAP DAN IMPLEMENTASI.....29
9.1 Tahap I: Persiapan dan Peletakan Fondasi (2025 – 2026).....30
9.2 Tahap II: Pengembangan dan Pembangunan Kapasitas (2027 – 2029).....31
9.3 Tahap III: Operasional Penuh dan Modernisasi Berkelanjutan (2030 dan Seterusnya).....33

BAB 10: RISIKO DAN MITIGASI.....34
10.1 Risiko Tumpang Tindih Wewenang dan Friksi Antar Lembaga.....34
10.2 Risiko Penyalahgunaan Kekuasaan dan Operasi Informasi.....35
10.3 Risiko Pelanggaran Privasi Warga Negara.....36
10.4 Risiko Ketergantungan pada Teknologi Asing.....36

BAB 11: TATA KELOLA DAN EVALUASI.....37

11.1 Model Pemeriksaan Periodik.....37
11.2 Indikator Capaian Kinerja (KPI).....38

BAB 12: STUDI PERBANDINGAN INTERNASIONAL.....39

BAB 13: REFERENSI (DAFTAR PUSTAKA).....40
Regulasi & Dokumen Resmi (12).....40
Jurnal Ilmiah & Akademik (15).....41
White Paper & Laporan Industri Internasional (10).....42
Berita & Laporan Media (10).....42
Situs Resmi & Lainnya (5).....42
KESIMPULAN.....43
LANGKAH SELANJUTNYA.....44

BAB 1: RINGKASAN EKSEKUTIF

Dunia telah memasuki era baru peperangan, di mana kedaulatan sebuah negara tidak lagi hanya diukur dari penguasaan atas darat, laut, dan udara, tetapi juga atas ranah maya (*cyberspace*). Eskalasi ancaman siber yang semakin canggih dan terorganisir kini telah berevolusi dari sekadar tindak kriminal menjadi instrumen kekuatan negara yang dapat mengancam stabilitas dan pertahanan nasional. Laporan dari berbagai lembaga, baik nasional seperti Badan Siber dan Sandi Negara (BSSN) maupun internasional seperti NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), secara konsisten menunjukkan tren peningkatan serangan siber yang disponsori oleh negara (*state-sponsored attacks*) yang menargetkan infrastruktur informasi vital, sistem pertahanan, dan proses demokrasi [1, 3]. Ancaman ini tidak lagi terbatas pada pencurian data, melainkan telah berkembang menjadi spionase siber, sabotase infrastruktur kritis, dan perang informasi yang dirancang untuk mengerosi kepercayaan publik serta melumpuhkan kemampuan negara dari dalam [2].

Menghadapi realitas ancaman ini, postur pertahanan siber Indonesia yang saat ini bersifat reaktif dan terfragmentasi di berbagai lembaga tidak lagi memadai. Diperlukan sebuah langkah strategis untuk mengkonsolidasikan kapabilitas, doktrin, dan komando pertahanan siber ke dalam sebuah kekuatan yang terpadu, proaktif, dan memiliki daya gentar (*deterrence*).

Untuk itu, *whitepaper* ini mengajukan usulan pembentukan **Angkatan Siber Indonesia (ASI)** sebagai sebuah kekuatan militer profesional yang berfokus pada peperangan di ranah maya. Usulan ini mengkonseptualisasikan ASI sebagai komando utama (Kotama) operasional khusus di bawah komando Panglima Tentara Nasional Indonesia (TNI), atau sebagai matra keempat yang berdiri setara dengan Angkatan Darat, Angatan Laut, dan Angkatan Udara. Dokumen ini akan menjabarkan secara komprehensif mengenai:

1. **Urgensi strategis** pembentukan ASI berdasarkan analisis ancaman global dan nasional.

2. **Landasan hukum dan kebijakan** yang dapat menjadi payung hukum bagi eksistensi dan operasi ASI.

3. **Visi, misi, fungsi, dan arsitektur organisasi** ASI yang terintegrasi dengan ekosistem pertahanan dan keamanan nasional.

4. **Kebutuhan sumber daya manusia, teknologi, dan anggaran** untuk mewujudkan kekuatan siber yang andal.

5. **Peta jalan implementasi** yang realistis dan terukur.

Pembentukan ASI adalah sebuah keniscayaan untuk memastikan Indonesia tidak hanya mampu bertahan, tetapi juga memiliki keunggulan dalam menghadapi dinamika konflik abad ke-21, demi menjaga kedaulatan digital dan keutuhan Negara Kesatuan Republik Indonesia.

BAB 2: LATAR BELAKANG DAN URGENSI

Keputusan untuk membentuk sebuah angkatan militer baru harus didasarkan pada analisis mendalam terhadap perubahan lanskap ancaman dan kebutuhan strategis negara. Bab ini menguraikan faktor-faktor pendorong yang menjadikan pembentukan Angkatan Siber Indonesia (ASI) sebagai sebuah kebutuhan yang mendesak.

2.1 Ancaman *Cyber Warfare* di Tingkat Global dan Nasional

Peperangan modern telah terbukti tidak dapat dipisahkan dari dimensi siber. Konflik global terkini, seperti yang terjadi di Ukraina, telah menjadi laboratorium hidup yang mempertontonkan bagaimana operasi siber digunakan secara masif dan efektif untuk mendukung tujuan militer konvensional. Serangan terhadap jaringan satelit, infrastruktur energi, sistem perbankan, dan diseminasi disinformasi yang sistematis telah menjadi bagian integral dari strategi perang [44]. Laporan dari Mandiant M-Trends 2024 menunjukkan bahwa kelompok *Advanced Persistent Threat* (APT) yang berafiliasi dengan negara semakin agresif menargetkan sektor pemerintahan dan infrastruktur kritis di seluruh dunia [6].

Bagi Indonesia, tren ini membawa implikasi langsung. Dengan posisi geopolitik yang strategis di Indo-Pasifik dan pertumbuhan ekonomi digital terbesar di Asia Tenggara, Indonesia adalah target yang sangat menarik.

Ancaman tidak hanya datang dari aktor non-negara atau kriminal siber, tetapi juga dari entitas negara yang memiliki tujuan spionase, sabotase ekonomi, atau bahkan persiapan untuk konflik di masa depan. Konseptualisasi perang siber dalam konteks pertahanan Indonesia harus berevolusi dari sekadar pertahanan jaringan menjadi sebuah doktrin yang utuh, yang mencakup aspek intelijen, pertahanan aktif, hingga kemampuan ofensif yang terukur sebagai bagian dari daya gentar nasional [4, 5].

2.2 Rentannya Pertahanan Siber Nasional: Studi Kasus di Indonesia

Selama beberapa tahun terakhir, Indonesia telah mengalami serangkaian insiden siber berskala besar yang mengekspos kerentanan fundamental dalam postur keamanan siber nasional. Menurut laporan BSSN, terjadi ratusan juta anomali trafik dan puluhan ribu insiden siber setiap tahunnya [7, 10]. Sejak 2019, lebih dari 70 kasus kebocoran data signifikan yang menimpa institusi pemerintah, BUMN, dan perusahaan swasta telah menjadi sorotan publik. Insiden seperti bocornya data pemilih dari Komisi Pemilihan Umum (KPU) tidak hanya melanggar hak privasi warga negara, tetapi juga berpotensi mengancam legitimasi proses demokrasi [8].

Namun, insiden yang terlihat di permukaan ini hanyalah puncak dari gunung es. Ancaman yang lebih tersembunyi dan berbahaya, seperti operasi APT yang menargetkan jaringan internal Kementerian Pertahanan, Mabes TNI, dan industri strategis, seringkali berlangsung tanpa terdeteksi dalam waktu lama. Serangan-serangan ini bertujuan mencuri data intelijen, desain alutsista, dan memetakan infrastruktur kritis untuk kemungkinan sabotase di masa depan. Kegagalan untuk melindungi data sensitif ini, meskipun Indonesia telah memiliki UU Pelindungan Data Pribadi [9], menunjukkan adanya celah antara regulasi dan kapabilitas teknis-operasional untuk menanganinya.

2.3 Perkembangan Regulasi: Celah dalam Aspek Pertahanan Militer

Pemerintah Indonesia telah menunjukkan keseriusan dalam memperkuat tata kelola keamanan siber melalui penerbitan Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber [10], yang kemudian diturunkan menjadi Peraturan BSSN No. 1 dan 2 Tahun 2024 [11,

12]. Regulasi ini menjadi landasan penting untuk sinergi antar lembaga dalam melindungi infrastruktur informasi vital dan mengelola krisis siber.

Meskipun demikian, fokus utama dari kerangka regulasi yang ada saat ini adalah pada aspek *governance*, koordinasi sipil, dan perlindungan. Belum ada regulasi yang secara eksplisit dan komprehensif mengatur domain siber sebagai sebuah mandala perang (*theatre of war*). Aspek pertahanan siber militer, operasi siber ofensif sebagai pilihan strategis, doktrin penggunaan kekuatan siber, serta aturan pelibatan (*rules of engagement*) dalam konflik siber belum terdefinisi secara jelas [13]. Celah inilah yang perlu diisi oleh sebuah entitas militer khusus, yang operasinya didasarkan pada doktrin pertahanan negara, bukan sekadar tata kelola keamanan informasi.

2.4 Fragmentasi Kelembagaan: Tumpang Tindih dan Celah Koordinasi

Saat ini, tanggung jawab keamanan siber Indonesia terdistribusi di beberapa lembaga dengan mandat yang berbeda. BSSN berperan sebagai koordinator keamanan siber nasional dan pelindung infrastruktur sipil [15]. Dittipidsiber Bareskrim Polri fokus pada penegakan hukum terhadap kejahatan siber. Di lingkungan pertahanan, terdapat Badan Informasi dan Komunikasi Pertahanan (Bainfokomhan) di bawah Kementerian Pertahanan yang mengurusi infrastruktur TIK pertahanan [16], serta unit-unit siber internal di setiap matra TNI (Siberad, Siber AL, Siberau).

Struktur yang terfragmentasi ini, meskipun dimaksudkan untuk pembagian tugas yang jelas, menciptakan tantangan serius dalam menghadapi ancaman siber bereskalasi tinggi. Sebuah serangan siber yang disponsori negara terhadap infrastruktur kritis nasional akan mengaburkan batas antara insiden sipil, tindak kriminal, dan serangan militer. Dalam situasi seperti ini, pertanyaan mendasar seperti "Siapa yang memegang komando respons?", "Kapan sebuah insiden dianggap sebagai tindakan perang?", dan "Siapa yang berwenang melakukan serangan balasan?" menjadi sulit dijawab dengan cepat. Tumpang tindih kewenangan ini berpotensi menyebabkan kelambatan respons, kebingungan komando, dan inefisiensi pengerahan sumber daya pada saat kritis [14].

2.5 Pelajaran dari Komunitas Internasional

Negara-negara maju telah lama menyadari bahwa ranah siber adalah domain operasional militer yang setara dengan domain lainnya. Amerika Serikat membentuk US Cyber Command (USCYBERCOM) sebagai salah satu dari sebelas *unified combatant commands*. Singapura secara resmi melantik Digital and Intelligence Service (DIS) sebagai matra keempat angkatan bersenjatanya pada tahun 2022 [30]. Jerman juga memiliki Cyber and Information Domain Service (KdoCIR) sebagai cabang militer independen [31].

Pendekatan ini menunjukkan sebuah konsensus internasional: kapabilitas siber yang efektif—baik defensif maupun ofensif—harus diintegrasikan secara penuh ke dalam struktur komando militer. Hal ini memungkinkan adanya kesatuan komando, pengembangan doktrin yang jelas, alokasi anggaran yang terfokus, dan jalur karier yang profesional bagi para prajurit siber. Dengan membentuk ASI, Indonesia akan mengikuti jejak praktik terbaik global, memastikan bahwa postur pertahanannya tetap relevan dan mampu memberikan efek gentar di panggung internasional, sambil mengadopsi kerangka kerja dan standar matang seperti yang dikeluarkan oleh NIST dan CMMI [17, 19].

BAB 3: LANDASAN HUKUM DAN KEBIJAKAN

Pembentukan Angkatan Siber Indonesia (ASI) sebagai kekuatan militer bukanlah sebuah tindakan yang berdiri dalam kekosongan hukum (*legal vacuum*). Sebaliknya, usulan ini berakar pada kerangka hukum pertahanan negara yang sudah ada dan dapat diperkuat melalui instrumen hukum baru yang spesifik. Bab ini akan menguraikan fondasi yuridis dan kebijakan yang menjadi dasar pembentukan, serta prinsip-prinsip yang akan memandu operasinya agar sejalan dengan hukum nasional dan internasional.

3.1 Landasan Yuridis Nasional: Undang-Undang dan Peraturan Presiden

Eksistensi dan tugas ASI dapat diturunkan dari beberapa peraturan perundang-undangan yang berlaku saat ini, yang secara kolektif memberikan

mandat kepada negara untuk melindungi segenap tumpah darah Indonesia, termasuk di ranah maya.

1. **Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara [20]:** UU ini adalah landasan utama. Pasal 1 ayat 1 menyatakan bahwa pertahanan negara adalah "segala usaha untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara." Di era digital, "ancaman dan gangguan" ini secara nyata telah meluas ke ranah siber. Dengan demikian, pembentukan kekuatan siber yang mampu mempertahankan kedaulatan digital adalah implementasi langsung dari amanat UU ini. Konsep Sistem Pertahanan dan Keamanan Rakyat Semesta (Sishankamrata) yang dianut juga relevan, di mana ASI akan menjadi komponen utama, dan masyarakat (talenta siber) menjadi komponen cadangan dan pendukung.

2. **Undang-Undang No. 34 Tahun 2004 tentang Tentara Nasional Indonesia [21]:** UU ini mendefinisikan tugas pokok TNI, yaitu menegakkan kedaulatan negara, mempertahankan keutuhan wilayah NKRI, serta melindungi segenap bangsa dan seluruh tumpah darah Indonesia dari ancaman dan gangguan. Ancaman siber berskala negara secara langsung menantang ketiga tugas pokok tersebut. Pembentukan ASI dapat dipandang sebagai modernisasi dan adaptasi struktur TNI untuk menjawab hakikat ancaman abad ke-21. ASI dapat dibentuk melalui revisi UU ini untuk menambahkannya sebagai matra keempat, atau melalui Peraturan Presiden sebagai Komando Utama (Kotama) Operasional baru di bawah Panglima TNI.

3. **Undang-Undang No. 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional (PSDN) untuk Pertahanan Negara [22]:** UU ini menyediakan payung hukum yang kuat untuk konsep "Komponen Cadangan Digital". Pasal 28 memungkinkan mobilisasi warga negara yang memiliki keahlian khusus untuk menjadi bagian dari Komponen Cadangan. Ini adalah landasan legal untuk merekrut para talenta siber terbaik dari kalangan sipil—seperti *ethical hackers*, akademisi, dan praktisi industri—untuk dilatih dan didayagunakan secara resmi bagi kepentingan pertahanan siber nasional.

4. **Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional [10]:** Perpres ini berfungsi sebagai payung strategis. Meskipun

menempatkan BSSN sebagai koordinator utama, dokumen ini menggarisbawahi pentingnya "peningkatan kapasitas dan kapabilitas pertahanan siber" sebagai salah satu pilar strategis. ASI akan menjadi ujung tombak implementasi pilar pertahanan tersebut, mengisi peran yang tidak dapat dijalankan oleh lembaga sipil, yaitu aspek pertahanan militer dan proyeksi kekuatan siber untuk menciptakan efek gentar.

Walaupun peraturan-peraturan di atas menyediakan dasar yang kuat, untuk memberikan kepastian hukum, alokasi anggaran yang permanen, dan kejelasan rantai komando, pembentukan ASI idealnya dikukuhkan melalui sebuah **Undang-Undang baru tentang Angkatan Siber Indonesia** atau setidaknya **Peraturan Presiden** yang secara khusus mengatur tentang pembentukannya sebagai Kotama Operasional TNI.

3.2 Kepatuhan pada Hukum Internasional: Prinsip dalam *Cyber Warfare*

Operasi ASI tidak akan berlangsung di "Wild West" digital. Sebagai instrumen negara, seluruh tindakannya harus tunduk pada hukum internasional, khususnya Hukum Humaniter Internasional (HHI) atau *Law of Armed Conflict* (LOAC). Panduan utama dalam menafsirkan penerapan HHI di ranah siber adalah **Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations**, yang disusun oleh para ahli hukum internasional terkemuka di bawah naungan NATO CCDCOE [26].

ASI harus beroperasi di bawah prinsip-prinsip HHI berikut:

- **Prinsip Pembedaan (*Distinction*):** Personel ASI harus mampu dan wajib membedakan antara target militer yang sah (seperti jaringan komando dan kontrol musuh, sistem senjata siber, atau infrastruktur yang digunakan untuk tujuan militer) dengan objek sipil yang dilindungi (seperti jaringan rumah sakit, sistem perbankan sipil, atau basis data kependudukan). Serangan yang sengaja menargetkan objek sipil adalah kejahatan perang.

- **Prinsip Proporsionalitas (*Proportionality*):** Setiap operasi siber ofensif harus dinilai secara cermat. Kerusakan ikutan (*collateral damage*) terhadap objek atau populasi sipil yang mungkin timbul tidak boleh berlebihan jika

dibandingkan dengan keuntungan militer konkret dan langsung yang diharapkan dari serangan tersebut.

- **Prinsip Kehati-hatian (*Precaution*):** Komandan ASI wajib mengambil semua tindakan pencegahan yang mungkin dilakukan untuk menghindari atau meminimalkan korban dan kerusakan sipil. Ini termasuk melakukan verifikasi target, memilih "senjata" siber dengan efek paling presisi, dan memberikan peringatan efektif jika memungkinkan.

Kepatuhan pada prinsip-prinsip ini tidak hanya merupakan kewajiban hukum, tetapi juga sebuah keharusan strategis untuk menjaga legitimasi Indonesia di mata komunitas internasional dan mencegah eskalasi konflik yang tidak terkendali [27, 28].

3.3 Perbandingan dan Praktik Terbaik (*Best Practices*) Internasional

Usulan pembentukan ASI sejalan dengan tren global dan mengadopsi pelajaran dari negara-negara yang telah lebih dulu mengembangkan kekuatan siber militer mereka.

- **Amerika Serikat - US Cyber Command (USCYBERCOM):** Pelajaran utama dari model AS adalah efektivitas struktur **komando tempur gabungan (*unified combatant command*)**. Model ini menempatkan satu komandan bintang empat yang bertanggung jawab atas seluruh operasi siber di Departemen Pertahanan, memberinya otoritas untuk menyinkronkan operasi siber Angkatan Darat, Laut, Udara, dan Marinir, serta mengintegrasikannya secara langsung ke dalam perencanaan perang nasional [29].

- **Singapura - Digital and Intelligence Service (DIS):** Model Singapura menawarkan pelajaran tentang **integrasi holistik**. DIS tidak hanya menangani pertahanan atau serangan siber, tetapi juga menggabungkan fungsi intelijen, perang psikologis, dan keamanan informasi dalam satu atap [30]. Pendekatan ini mengakui bahwa peperangan modern adalah tentang penguasaan domain informasi secara menyeluruh, bukan hanya aspek teknis peretasan.

- **Jerman - Cyber and Information Domain Service (KdoCIR):** Praktik terbaik dari Jerman adalah komitmen pada **profesionalisasi melalui pembentukan matra khusus**. Dengan menjadikan kekuatan siber sebagai

cabang militer yang setara dengan yang lain, Jerman menciptakan jalur karier yang jelas, budaya organisasi yang unik, serta pusat keunggulan dalam riset dan doktrin yang berfokus murni pada domain siber dan informasi [31].

Dengan demikian, landasan hukum untuk ASI sudah tersedia, kerangka kepatuhan internasionalnya jelas, dan model organisasinya dapat dirancang dengan mengacu pada praktik terbaik yang telah terbukti efektif di negara lain. Ini memberikan fondasi yang kokoh untuk melangkah ke tahap selanjutnya, yaitu perancangan visi, misi, dan struktur organisasi.

BAB 4: VISI, MISI, DAN FUNGSI

Setiap organisasi militer yang efektif harus memiliki doktrin yang jelas, yang dimulai dari penetapan visi, misi, dan fungsi. Bagian ini merumuskan identitas dan tujuan dari Angkatan Siber Indonesia (ASI), yang akan menjadi pedoman bagi penyusunan struktur organisasi, pengembangan sumber daya, dan pelaksanaan operasi.

4.1 Visi

Visi Angkatan Siber Indonesia adalah:

"Menjaga kedaulatan digital Negara Kesatuan Republik Indonesia melalui kekuatan siber yang tangguh, adaptif, dan berdaya gentar tinggi."

Visi ini mengandung beberapa elemen kunci yang menjadi cita-cita tertinggi ASI:

- **Menjaga Kedaulatan Digital:** Visi ini menegaskan bahwa ranah siber adalah perluasan dari teritori kedaulatan negara. "Kedaulatan digital" bermakna bahwa Indonesia memiliki hak dan kemampuan untuk mengatur ruang sibernya, melindungi integritas data dan infrastruktur informasinya, serta bebas

dari paksaan atau intervensi aktor negara asing di ranah maya. Ini adalah manifestasi kedaulatan negara di abad ke-21.

- **Kekuatan yang Tangguh (*Resilient*):** "Tangguh" berarti kemampuan untuk tidak hanya menahan serangan, tetapi juga untuk terus beroperasi di bawah tekanan, memitigasi kerusakan, dan pulih dengan cepat. Ketangguhan ini dibangun dari sistem pertahanan berlapis, personel yang terlatih, dan prosedur respons insiden yang solid.

- **Adaptif (*Adaptive*):** Ranah siber dicirikan oleh perubahan teknologi dan taktik yang sangat cepat. ASI tidak boleh menjadi organisasi yang kaku dan birokratis. Sifat "adaptif" menuntut ASI untuk terus berinovasi, mengadopsi teknologi baru, memperbarui doktrin secara berkala, dan memiliki struktur organisasi yang fleksibel untuk merespons ancaman yang belum pernah ada sebelumnya.

- **Berdaya Gentar Tinggi (*High Deterrence*):** Ini adalah elemen sentral dari sebuah kekuatan militer. Daya gentar tidak hanya dicapai melalui pertahanan yang pasif, tetapi juga melalui kepemilikan kapabilitas ofensif yang kredibel. Potensi ancaman dari serangan siber Indonesia yang terukur dan menyakitkan harus mampu membuat calon agresor berpikir dua kali. Keberadaan ASI itu sendiri harus menjadi pesan strategis bahwa setiap serangan siber terhadap kepentingan nasional Indonesia akan menghadapi konsekuensi yang serius [33].

4.2 Misi

Untuk mewujudkan visi tersebut, Angkatan Siber Indonesia mengemban misi-misi strategis sebagai berikut:

1. **Menyelenggarakan Pertahanan Siber Militer:** Merancang, membangun, dan mengoperasikan sistem pertahanan siber untuk melindungi jaringan dan sistem senjata milik Tentara Nasional Indonesia (TNI). Selain itu, ASI bertindak sebagai benteng pertahanan terakhir (*defender of last resort*) bagi Infrastruktur Informasi Vital (IIV) nasional apabila terjadi serangan siber bereskalasi tinggi yang mengancam keamanan negara.

2. **Melaksanakan Operasi Intelijen Siber dan Sinyal:** Mengumpulkan, menganalisis, dan menyebarkan informasi intelijen dari ranah siber dan

spektrum elektromagnetik untuk memberikan peringatan dini terhadap ancaman, mendukung perencanaan operasi militer, dan memberikan keunggulan informasi bagi para pengambil keputusan strategis.

3. **Mengembangkan dan Melaksanakan Operasi Siber Ofensif:** Membangun kemampuan untuk melakukan operasi siber ofensif yang terukur dan terkalkulasi sebagai salah satu opsi bagi Panglima TNI dan Presiden dalam merespons agresi atau untuk mencapai tujuan keamanan nasional. Pelaksanaan operasi ini harus dilakukan di bawah otorisasi yang ketat dan sejalan dengan hukum nasional maupun internasional.

4. **Melaksanakan Operasi Informasi Strategis:** Melindungi ruang informasi nasional dari kampanye disinformasi, misinformasi, dan propaganda yang dilancarkan oleh aktor negara asing. Selain itu, ASI juga bertugas melaksanakan operasi informasi untuk membentuk persepsi di ranah digital demi mendukung pencapaian tujuan strategis Indonesia.

5. **Membina dan Mendayagunakan Sumber Daya Nasional di Ranah Siber:** Membangun sistem pembinaan sumber daya manusia siber yang unggul, baik dari jalur militer maupun sipil melalui mekanisme Komponen Cadangan. ASI bertanggung jawab untuk menetapkan standar kompetensi, menyelenggarakan pelatihan, dan menciptakan jalur karier yang jelas bagi para prajurit siber [32].

4.3 Fungsi Inti

Untuk menjalankan misinya, ASI akan distrukturkan ke dalam beberapa unit fungsional utama. Meskipun nama dan struktur detailnya akan diatur lebih lanjut, fungsi-fungsi inti dari ASI adalah sebagai berikut:

- **Cyber Defense Command (CDC) / Komando Pertahanan Siber:** Bertindak sebagai "perisai" negara di ranah maya. Unit ini bertanggung jawab untuk operasi pertahanan aktif (*active defense*), pemantauan jaringan kritis secara 24/7, perburuan ancaman (*threat hunting*), dan respons insiden siber pada jaringan militer dan infrastruktur kritis nasional yang ditetapkan.

- **Cyber Attack Unit (CAU) / Satuan Serangan Siber:** Bertindak sebagai "tombak" negara. Unit ini terdiri dari para operator siber berkemampuan tinggi yang bertugas merencanakan dan mengeksekusi operasi siber ofensif sesuai

perintah dari rantai komando. Aktivitasnya bersifat rahasia dan berada di bawah pengawasan yang sangat ketat.

- **Digital Intelligence Battalion (DIB) / Batalyon Intelijen Digital:** Bertindak sebagai "mata dan telinga". Unit ini adalah tulang punggung intelijen bagi CDC dan CAU. Tugasnya mencakup *malware reverse engineering*, analisis forensik digital, intelijen sinyal (SIGINT), dan analisis *open-source intelligence* (OSINT) untuk memetakan kekuatan, kelemahan, dan intensi lawan.

- **Information Operations Directorate (INO) / Direktorat Operasi Informasi:** Bertindak sebagai "suara" strategis. Unit ini fokus pada aspek kognitif dari peperangan informasi. Fungsinya meliputi analisis sentimen media sosial, kontra-propaganda, diseminasi narasi strategis, dan pelaksanaan *psychological operations* (psyops) di ranah digital.

- **Pusat Pembinaan Komponen Cadangan Digital (Pusbin Komcad Digital):** Bertindak sebagai "kawah candradimuka". Unit ini bertanggung jawab atas seluruh siklus manajemen talenta sipil: mulai dari identifikasi dan rekrutmen talenta siber dari universitas dan industri, pelaksanaan pendidikan dasar kemiliteran, pelatihan teknis lanjutan sesuai standar ASI, hingga mekanisme mobilisasi saat dibutuhkan.

BAB 5: STRUKTUR ORGANISASI DAN KOORDINASI

Struktur organisasi yang efektif dan model koordinasi yang jelas adalah kunci untuk menghindari tumpang tindih kewenangan dan memastikan Angkatan Siber Indonesia (ASI) dapat beroperasi secara cepat dan terpadu. Bab ini mengusulkan posisi strategis ASI dalam arsitektur pertahanan nasional, serta mekanisme kerjasamanya dengan lembaga-lembaga terkait.

5.1 Posisi dan Struktur Komando

Untuk memastikan kecepatan implementasi dan integrasi yang mulus ke dalam doktrin pertahanan yang ada, model yang paling pragmatis untuk pembentukan awal ASI adalah sebagai **Komando Utama Operasional (Kotama Ops)**.

Posisi: Angkatan Siber Indonesia (ASI) diusulkan untuk dibentuk sebagai sebuah **Komando Utama Operasional (Kotama Ops) yang berkedudukan langsung di bawah Panglima Tentara Nasional Indonesia (TNI)**.

Status ini menempatkan ASI setara dengan Kotama Ops lainnya, seperti Komando Cadangan Strategis Angkatan Darat (Kostrad), Komando Armada RI (Koarmada RI), Komando Operasi Udara Nasional (Koopsudnas), dan Komando Gabungan Wilayah Pertahanan (Kogabwilhan). Posisi ini memberikan beberapa keuntungan strategis:

1. **Kesatuan Komando:** Panglima ASI melapor langsung kepada Panglima TNI, memastikan bahwa pengerahan kekuatan siber selaras dengan strategi militer nasional secara keseluruhan.

2. **Otoritas Gabungan:** Sebagai Kotama Ops, ASI memiliki wewenang untuk merencanakan dan melaksanakan operasi siber yang bersifat gabungan (melibatkan tiga matra).

3. **Fleksibilitas Implementasi:** Pembentukan Kotama Ops dapat dilakukan melalui Peraturan Presiden (Perpres) atau bahkan Peraturan Panglima TNI, sebuah proses yang lebih cepat dibandingkan harus mengamandemen UU No. 34/2004 untuk menciptakan matra keempat.

Struktur Komando: ASI akan dipimpin oleh seorang Panglima (Pang-ASI) dengan pangkat bintang tiga (Letnan Jenderal, Laksamana Madya, atau Marsekal Madya) untuk menjamin bobot otoritas yang setara saat berkoordinasi dengan para kepala staf angkatan.

Secara visual, struktur komando dapat digambarkan sebagai berikut:

- **Puncak Komando:** Panglima TNI
  - **Komando Langsung: Panglima Angkatan Siber Indonesia (Pang-ASI)**

- **Staf & Unsur Pelayanan:**

1. Inspektorat ASI
2. Staf Perencanaan & Anggaran
3. Staf Intelijen
4. Staf Operasi
5. Staf Personalia
6. Staf Logistik

- **Unit Fungsional / Komando Pelaksana (di bawah Pang-ASI):**

1. Komando Pertahanan Siber (CDC)
2. Satuan Serangan Siber (CAU)
3. Batalyon Intelijen Digital (DIB)
4. Direktorat Operasi Informasi (INO)
5. Pusat Pembinaan Komponen Cadangan Digital (Pusbin Komcad Digital)

Garis komando yang vertikal dan tegas ini memastikan bahwa seluruh kapabilitas siber militer berada di bawah satu atap, menghilangkan ambiguitas dan mempercepat proses pengambilan keputusan.

5.2 Peran dan Tugas Tiap Unit

Peran dan tugas pokok dari masing-masing unit fungsional inti ASI (CDC, CAU, DIB, INO, dan Pusbin Komcad Digital) telah dijabarkan secara rinci pada **Bab 4.3**. Struktur komando ini menegaskan bahwa kelima unit tersebut merupakan

komando pelaksana di bawah kendali operasional penuh Panglima ASI, yang kemudian bertanggung jawab kepada Panglima TNI. Hal ini menjamin prinsip *unity of command and unity of effort* dalam setiap operasi siber yang dilaksanakan.

5.3 Model Koordinasi Antar Lembaga

Pembentukan ASI **tidak bertujuan untuk mengambil alih atau menggantikan** peran lembaga siber yang sudah ada. Sebaliknya, ASI dirancang untuk mengisi celah pada spektrum pertahanan dan keamanan tingkat militer. Kunci keberhasilannya terletak pada model koordinasi yang jelas, yang terinspirasi dari praktik terbaik internasional seperti model *National Cyber Security Centre* (NCSC) di Inggris [34].

Berikut adalah model koordinasi yang diusulkan:

- **Badan Siber dan Sandi Negara (BSSN):** Tetap menjadi **Koordinator Keamanan Siber Nasional** dan **CSIRT Nasional** untuk sektor sipil, pemerintah, dan Infrastruktur Informasi Vital (IIV). BSSN adalah "pintu gerbang" utama untuk pelaporan dan respons awal terhadap semua insiden siber. Ketika sebuah insiden teridentifikasi memiliki skala, atribusi, dan dampak yang mengancam stabilitas nasional (misalnya, serangan oleh aktor negara), BSSN, sesuai amanat Perpres 47/2023, bertanggung jawab untuk mengoordinasikan manajemen krisis siber dan memberikan rekomendasi eskalasi kepada pimpinan nasional.

- **Angkatan Siber Indonesia (ASI):** Berfungsi sebagai **penerima eskalasi ancaman berdimensi militer**. Mandat operasional ASI dimulai ketika sebuah ancaman siber secara resmi dinyatakan sebagai ancaman terhadap pertahanan dan keamanan negara. Fokus ASI adalah pada:

1. Ancaman yang berasal dari aktor negara asing.

2. Serangan yang menargetkan sistem pertahanan dan komando nasional.

3. Serangan masif terhadap IIV yang dapat melumpuhkan negara.

4. Pelaksanaan operasi siber (termasuk ofensif) sebagai bagian dari respons negara.

- **Badan Intelijen Negara (BIN):** Berperan sebagai pemasok **intelijen strategis**. BIN memberikan analisis mengenai intensi, kebijakan, dan kapabilitas siber negara lain dari perspektif politik dan strategis. Intelijen dari BIN akan menjadi masukan krusial bagi DIB (Batalyon Intelijen Digital) milik ASI, yang fokus pada analisis teknis dan operasional. Perlu dibentuk sebuah sel fusi intelijen (*intelligence fusion cell*) antara BIN dan ASI.

- **Kepolisian Negara Republik Indonesia (Polri):** Tetap menjadi **lembaga penegak hukum utama** untuk tindak pidana siber (*cybercrime*). Jika sebuah serangan siber (misalnya *ransomware*) murni bermotif kriminal, penanganannya berada di bawah yurisdiksi Dittipidsiber Bareskrim Polri. Namun, dalam skenario serangan hibrida (misalnya, *ransomware* yang dilancarkan oleh aktor negara), akan ada koordinasi erat: Polri menangani aspek investigasi kriminal dan penegakan hukumnya, sementara ASI menangani aspek pertahanan nasional dan respons militer terhadap aktor negara tersebut.

Untuk meresmikan mekanisme ini, diusulkan pembentukan **Forum Koordinasi Keamanan Siber Nasional** yang dipimpin oleh Menteri Koordinator Bidang Politik, Hukum, dan Keamanan (Menko Polhukam). Forum ini beranggotakan Kepala BSSN, Panglima TNI, Kepala BIN, dan Kapolri. Forum ini bertemu secara berkala dan dalam situasi krisis untuk melakukan dekonfliksi, berbagi informasi intelijen, dan merekomendasikan opsi respons terpadu kepada Presiden. Model seperti ini sejalan dengan berbagai studi tentang tata kelola siber nasional yang efektif [35].

BAB 6: SUMBER DAYA DAN SUMBER DAYA MANUSIA (SDM)

Kekuatan sebuah angkatan siber tidak diukur dari jumlah server atau kecanggihan perangkat lunaknya, melainkan dari kualitas, keahlian, dan dedikasi para personelnya. Manusia adalah sistem senjata utama dalam peperangan siber. Oleh karena itu, pembangunan Angkatan Siber Indonesia (ASI) harus menempatkan strategi akuisisi, pendidikan, dan pembinaan SDM sebagai prioritas tertinggi.

6.1 Kebutuhan SDM: Memburu Talenta Spesialis

Tantangan utama yang dihadapi Indonesia, dan juga dunia, adalah kesenjangan talenta siber (*cybersecurity skills gap*). Laporan (ISC)² Cybersecurity Workforce Study tahun 2023 menunjukkan adanya kekurangan jutaan tenaga profesional siber di tingkat global [36]. Di tingkat nasional, Kementerian Kominfo juga memproyeksikan kebutuhan ratusan ribu talenta digital setiap tahunnya untuk mendukung ekonomi digital [37]. ASI akan berkompetisi di pasar yang sama untuk merekrut talenta-talenta terbaik.

Untuk menjadi kekuatan yang efektif, ASI tidak membutuhkan staf IT generalis, melainkan para spesialis dengan keahlian mendalam. Personel ASI harus merupakan perpaduan unik antara seorang "prajurit" yang disiplin dan patriotik dengan seorang "ilmuwan" yang memiliki ketajaman teknis. Beberapa peran krusial yang harus diisi antara lain:

- ***Ethical Hackers / Penetration Testers:*** Menjadi tulang punggung Satuan Serangan Siber (CAU) untuk operasi ofensif, sekaligus berperan sebagai *Red Team* yang secara rutin menguji dan memperkuat pertahanan Komando Pertahanan Siber (CDC).

- ***Malware Reverse Engineers:*** Ujung tombak Batalyon Intelijen Digital (DIB) yang bertugas "membedah" perangkat lunak jahat (malware) musuh untuk memahami cara kerjanya, dari mana asalnya, dan bagaimana mengembangkan penangkalnya.

- ***Threat Hunters:*** Operator proaktif di dalam CDC yang tidak menunggu alarm berbunyi. Mereka secara aktif menjelajahi jaringan untuk mencari jejak-jejak penyusup (*Indicators of Compromise*) berdasarkan hipotesis bahwa jaringan mungkin telah ditembus.

- ***Data Scientists & AI Specialists:*** Menganalisis volume data yang masif dari lalu lintas jaringan dan sumber intelijen lainnya untuk mengidentifikasi pola serangan, mendeteksi anomali, serta melacak dan memitigasi kampanye disinformasi yang dilancarkan oleh Direktorat Operasi Informasi (INO).

- ***SIGINT & CNO Analysts (Signals Intelligence & Computer Network Operations):*** Menerjemahkan kemampuan intelijen sinyal klasik ke dunia digital,

dengan fokus pada penyadapan, dekripsi, dan analisis komunikasi serta operasi jaringan yang dilakukan oleh pihak lawan.

- ***Quantum Computing & Cryptography Researchers:*** Sebagai unit riset berwawasan ke depan, mereka bertugas meneliti dampak komputasi kuantum terhadap kriptografi modern dan mempersiapkan Indonesia untuk era kriptografi pasca-kuantum (*post-quantum cryptography*), menjamin keamanan informasi negara dalam jangka panjang.

6.2 Pendidikan dan Pelatihan: Membangun Pipa Regenerasi dari Hulu ke Hilir

Mencetak SDM dengan kualitas di atas tidak bisa dilakukan secara instan. Diperlukan sebuah sistem pendidikan dan pelatihan yang terintegrasi dari hulu hingga hilir.

1. **Hulu (Penjaringan Bakat Sejak Dini):**

   - **Tingkat Sekolah & Universitas:** ASI perlu bekerja sama dengan Kemendikbudristek untuk mempromosikan minat pada keamanan siber sejak SMA/SMK melalui ekstrakurikuler, klub siber, dan kompetisi. Di tingkat perguruan tinggi, ASI harus menjalin kemitraan strategis dengan kampus-kampus unggulan seperti ITB, UI, UGM, ITS, serta secara khusus dengan Universitas Pertahanan (UNHAN) [39]. Kemitraan ini dapat berupa beasiswa ikatan dinas, pengembangan kurikulum pertahanan siber, dan rekrutmen langsung dari lulusan terbaik.

2. **Tengah (Pendidikan & Pelatihan Formal):**

   - **Akademi Militer & Pendidikan Pertama:** Kurikulum pertahanan siber harus menjadi bagian wajib bagi seluruh taruna di Akmil, AAL, dan AAU.

Selanjutnya, perlu dibentuk sebuah kecabangan atau korps khusus Siber, di mana para taruna terpilih akan mendapatkan pendidikan lanjutan yang mendalam.

○ **Pusat Pendidikan Siber TNI:** ASI harus memiliki pusat pendidikan dan latihan (Pusdiklat) khusus yang menjadi kawah candradimuka bagi semua prajurit siber. Pusdiklat ini menyelenggarakan pendidikan dasar, spesialisasi, hingga kursus-kursus lanjutan yang disesuaikan dengan perkembangan ancaman. Latihan-latihan gabungan siber seperti yang sudah pernah digelar TNI [38] harus ditingkatkan frekuensi dan kompleksitasnya.

3. **Hilir (Pengembangan Berkelanjutan & Uji Kemampuan):**

○ **Kompetisi & Sertifikasi:** Keterampilan siber bersifat mudah rusak (*perishable*). Untuk menjaga ketajamannya, personel ASI wajib mengikuti kompetisi *Capture The Flag* (CTF) secara rutin, baik di tingkat nasional maupun internasional [40]. Selain itu, mereka harus didorong dan didanai untuk meraih sertifikasi profesional yang diakui secara global (misalnya, OSCP, CISSP, GCIH, dsb.) sebagai standar kompetensi.

6.3 Pola Rekrutmen dan Kerja Sama Internasional

Menyadari bahwa talenta siber terbaik tersebar di berbagai sektor, ASI harus mengadopsi model rekrutmen yang fleksibel dan terbuka.

- **Rekrutmen Jalur Ganda (*Dual-Track Recruitment*):**

○ **Jalur Karier Militer:** Melalui jalur pendidikan perwira (Akmil, Sepa PK), bintara, dan tamtama reguler untuk membentuk tulang punggung organisasi yang berdisiplin militer.

○ **Jalur Sumber Eksternal (Sipil):** Ini adalah jalur krusial untuk mengakuisisi keahlian teknis yang langka.

- **Komponen Cadangan Digital:** Merekrut profesional dari industri swasta, akademisi, dan komunitas *ethical hacker* melalui mekanisme PSDN [22]. Mereka akan diberikan pelatihan militer dasar dan dapat dimobilisasi saat negara membutuhkan.

- **Rekrutmen Khusus Perwira Prajurit Karier (Pa PK):** Membuka jalur khusus bagi WNI dengan kualifikasi istimewa (misal, lulusan S2/S3 bidang *cybersecurity*, pemenang kompetisi siber internasional, atau peneliti dengan rekam jejak terbukti) untuk dapat langsung menjadi perwira di ASI.

- **Kerja Sama Internasional:** Ancaman siber bersifat lintas batas, sehingga pertahanannya pun harus kolaboratif. ASI harus secara proaktif menjalin kerja sama dengan angkatan siber negara-negara sahabat.

  - **Latihan Bersama:** Mengirimkan tim untuk berpartisipasi dalam latihan siber internasional bergengsi seperti *Locked Shields* (NATO), *Cyber Flag* (AS), atau *Talent Search* (Jepang).

  - **Pertukaran Personel dan Pendidikan:** Mengirimkan perwira-perwira terbaik ASI untuk menempuh pendidikan di lembaga siber militer negara mitra seperti AS, Australia, Singapura, Korea Selatan, atau Inggris [41]. Sebaliknya, menerima perwira mereka untuk berbagi pengalaman. Program ini adalah cara paling efektif untuk transfer pengetahuan, doktrin, dan membangun interoperabilitas.

BAB 7: KAPABILITAS TEKNIS DAN INFRASTRUKTUR

Sumber daya manusia yang unggul harus ditopang oleh teknologi dan infrastruktur yang superior. Untuk dapat menjalankan spektrum operasinya secara efektif, Angkatan Siber Indonesia (ASI) harus membangun dan menguasai serangkaian kapabilitas teknis yang modern, mandiri, dan berketahanan tinggi. Fondasi teknologi ini adalah otot yang akan menggerakkan otak para prajurit siber.

7.1 Pilar Kapabilitas Teknis

Pembangunan kapabilitas teknis ASI akan berpusat pada lima pilar utama yang saling mendukung, dari pertahanan dasar hingga penguasaan teknologi masa depan.

1. **Deteksi dan Respons Canggih (CIRT Militer):** Fondasi dari semua operasi pertahanan adalah kemampuan untuk melihat dan merespons. ASI harus memiliki *Computer Emergency Response Team* (CIRT) atau *Security Operations Center* (SOC) khusus militer yang beroperasi 24/7. Berbeda dengan CSIRT Nasional (Id-SIRTII/CC) yang melayani publik [42], CIRT militer ini dirancang untuk menangani ancaman tingkat tinggi dengan fitur:

   - **Teknologi Terkini:** Dilengkapi dengan platform *Security Information and Event Management* (SIEM), *Security Orchestration, Automation, and Response* (SOAR), *Endpoint Detection and Response* (EDR), dan *Network Detection and Response* (NDR) kelas militer.

   - ***Cyber Range*:** Sebuah laboratorium siber atau arena tempur virtual yang canggih. *Cyber Range* berfungsi sebagai fasilitas untuk melakukan simulasi serangan, menguji ketahanan sistem, melatih operator dalam skenario realistis, serta menguji "senjata" siber baru tanpa membahayakan jaringan aktif.

2. **Kapabilitas Siber Ofensif yang Mandiri:** Daya gentar tidak akan tercipta tanpa kemampuan untuk "membalas". ASI harus memiliki kapabilitas siber ofensif yang mandiri untuk mengurangi ketergantungan pada teknologi asing. Unit ini, yang berada di bawah pengawasan sangat ketat, bertanggung jawab untuk:

   - **Riset Kerentanan (*Vulnerability Research*):** Secara proaktif meneliti dan menemukan kerentanan baru (*zero-day vulnerabilities*) pada sistem yang digunakan oleh musuh potensial.

   - **Pengembangan *Exploit* & *Payload*:** Mengembangkan sendiri perangkat lunak yang digunakan untuk operasi ofensif, yang disesuaikan dengan target

spesifik dan tujuan misi. Kemandirian ini krusial untuk menjamin kerahasiaan dan efektivitas operasi.

3. **Platform Perang Informasi (*Information Warfare*):** Untuk mendukung Direktorat Operasi Informasi (INO), diperlukan sebuah platform teknologi yang mampu mengolah dan menganalisis samudera informasi digital. Platform ini harus mampu:

   - **Analisis *Big Data* dan Sentimen:** Menggunakan kecerdasan buatan untuk memonitor media sosial, portal berita, dan forum daring secara *real-time* guna memetakan narasi, mengukur sentimen publik, dan mendeteksi anomali.

   - **Deteksi dan Atribusi Disinformasi:** Mengidentifikasi kampanye disinformasi yang terkoordinasi, melacak sumbernya, mengidentifikasi jaringan bot, dan memberikan data untuk operasi kontra-propaganda.

4. **Kecerdasan Buatan (AI) sebagai Pengganda Kekuatan:** AI bukan lagi fiksi ilmiah, melainkan kebutuhan operasional. Sesuai tren global yang dilaporkan oleh Gartner [43], AI akan diintegrasikan di seluruh lini kapabilitas ASI:

   - **AI untuk Pertahanan:** Menggunakan *machine learning* untuk mendeteksi pola serangan baru (malware polimorfik, anomali perilaku) yang tidak terdeteksi oleh antivirus tradisional.

   - **AI untuk Intelijen:** Mengotomatiskan analisis data intelijen dalam jumlah besar untuk menemukan hubungan tersembunyi dan mempercepat pengambilan keputusan.

   - **AI untuk Operasi Informasi:** Meningkatkan kemampuan analisis sentimen dan deteksi *deepfake* yang digunakan dalam propaganda musuh.

5. **Riset Kriptografi Kuantum:** Ini adalah pilar untuk memastikan supremasi informasi Indonesia di masa depan. Kemunculan komputer kuantum mengancam akan mematahkan hampir semua sistem enkripsi yang kita

gunakan saat ini. Sesuai dengan Rencana Strategis Kementerian Pertahanan untuk penguasaan teknologi kunci [44], ASI harus menjadi pionir dalam:

- **Pengembangan Kriptografi Pasca-Kuantum (*Post-Quantum Cryptography* - PQC):** Meriset dan mengembangkan algoritma enkripsi baru yang tahan terhadap serangan baik dari komputer klasik maupun kuantum.
- **Implementasi Jaringan Komunikasi Aman:** Mempersiapkan transisi sistem komunikasi vital pemerintah dan militer ke standar PQC untuk melindungi rahasia negara dalam jangka panjang.

7.2 Penjaminan Keamanan *Vital Information Infrastructure* (VII)

ASI memiliki peran krusial namun spesifik dalam melindungi 11 sektor Infrastruktur Informasi Vital (IIV) nasional. Peran ini didasarkan pada model pertahanan berlapis (*layered defense*):

- **Lapis Pertama (Pemilik IIV):** Tanggung jawab utama keamanan siber berada di tangan setiap pengelola IIV (misalnya, PLN, Pertamina, perbankan).
- **Lapis Kedua (Koordinator Nasional - BSSN):** BSSN memberikan panduan, standar, bantuan teknis, dan koordinasi respons insiden untuk seluruh sektor IIV di ranah sipil.
- **Lapis Ketiga (Benteng Terakhir - ASI):** ASI akan diaktifkan untuk melindungi IIV hanya jika kondisi eskalasi terpenuhi, yaitu: (1) serangan memiliki skala dan kecanggihan yang melampaui kemampuan BSSN dan pemilik IIV, (2) serangan teratribusi kuat berasal dari aktor negara asing, dan (3) serangan tersebut berpotensi menyebabkan kelumpuhan nasional. Aktivasi peran ASI ini dilakukan atas perintah Presiden.

7.3 Kolaborasi Riset dan Pengembangan (R&D)

Untuk mengakselerasi penguasaan teknologi dan mengurangi ketergantungan impor, ASI harus menerapkan model inovasi "Helix Ganda" yang melibatkan kolaborasi erat antara pemerintah, akademisi, dan industri.

- **Kolaborasi Dalam Negeri:**

  - **BRIN:** Menjalin kerja sama riset fundamental dengan Badan Riset dan Inovasi Nasional (BRIN) di bidang-bidang strategis seperti AI dan komputasi kuantum [45].

  - **Perguruan Tinggi:** Membangun laboratorium riset bersama (*joint research labs*) dengan pusat-pusat keunggulan akademik (ITB, UGM, UI, ITS) untuk mengembangkan solusi spesifik dan menjaring talenta.

  - **Industri Pertahanan:** Bersinergi dengan industri pertahanan dalam negeri (PT. LEN Industri, PT. INTI, dll.) dan swasta untuk produksi massal perangkat keras dan lunak siber yang telah teruji, mewujudkan kemandirian alutsista siber.

- **Adopsi Standar Global:** Seluruh infrastruktur dan proses teknis ASI harus dibangun di atas fondasi standar internasional untuk menjamin kualitas, keamanan, dan interoperabilitas. Standar acuan utama meliputi **NIST Cybersecurity Framework** untuk manajemen risiko [28], **ISO/IEC 27001** untuk sistem manajemen keamanan informasi [46], dan **CMMI** untuk kematangan proses [29].

BAB 8: PENDANAAN DAN ANGGARAN

Membangun kekuatan siber yang kredibel adalah sebuah investasi strategis jangka panjang dengan kebutuhan biaya yang signifikan. Namun, biaya dari kelambanan atau ketiadaan kekuatan ini—yang diukur dari potensi kerugian ekonomi akibat sabotase, pencurian kekayaan intelektual, dan kelumpuhan infrastruktur kritis—jauh lebih besar. Bab ini menguraikan estimasi kebutuhan dan model pembiayaan untuk Angkatan Siber Indonesia (ASI).

8.1 Estimasi Kebutuhan Anggaran

Anggaran untuk ASI harus dipisahkan dari anggaran rutin matra lain untuk menjamin fokus dan akuntabilitas. Kebutuhan anggaran dapat dibagi menjadi dua kategori utama: Belanja Modal (*Capital Expenditure* - CAPEX) untuk pembangunan awal dan Belanja Operasional (*Operational Expenditure* - OPEX) untuk keberlangsungan operasi.

A. Belanja Modal (CAPEX) - Investasi Awal (Jangka Pendek-Menengah)

Ini adalah biaya yang diperlukan selama Tahap Persiapan dan Pengembangan (sekitar 5 tahun pertama) untuk membangun fondasi ASI. Komponen utamanya meliputi:

1. **Infrastruktur Fisik:** Pembangunan markas komando ASI yang memiliki standar keamanan tinggi (*secure facility*), pusat data (*data center*) Tier 3 atau Tier 4 yang mungkin ditempatkan di bawah tanah, serta Pusat Pendidikan dan Latihan (Pusdiklat) khusus siber.

2. **Infrastruktur Digital:** Pengadaan perangkat keras inti seperti *server farm*, *high-performance computing* (HPC) untuk analisis data, perangkat jaringan yang terenkripsi, dan pembangunan fasilitas *Cyber Range* yang komprehensif.

3. **Perangkat Keras dan Lunak:** Akuisisi ribuan unit komputer klien (*endpoints*) yang aman, perangkat analisis forensik, serta lisensi perangkat lunak esensial untuk *platform* SIEM, SOAR, intelijen ancaman, dan analisis *malware*.

4. **R&D dan Akuisisi Kapabilitas Awal:** Alokasi dana khusus untuk riset dan pengembangan awal yang dilakukan oleh Satuan Serangan Siber (CAU) dan Batalyon Intelijen Digital (DIB) untuk membangun basis data dan perangkat mula.

B. Belanja Operasional (OPEX) - Biaya Tahunan

Ini adalah biaya rutin yang diperlukan untuk menjaga agar ASI tetap beroperasi pada tingkat kesiapan tertinggi.

1. **Gaji dan Tunjangan Personel:** Ini akan menjadi komponen OPEX terbesar. Untuk menarik dan mempertahankan talenta siber terbaik yang juga menjadi incaran sektor swasta, perlu dirancang **skema remunerasi khusus** yang kompetitif. Gaji prajurit siber harus merefleksikan kelangkaan dan tingkat keahlian mereka.

2. **Pemeliharaan dan Lisensi:** Biaya tahunan untuk perpanjangan lisensi perangkat lunak, kontrak pemeliharaan perangkat keras, dan langganan data intelijen ancaman (*threat intelligence feeds*) dari berbagai vendor global.

3. **Riset dan Pengembangan Berkelanjutan:** Alokasi anggaran tahunan yang signifikan dan konsisten untuk R&D guna memastikan ASI tidak tertinggal dari laju perkembangan teknologi dan taktik musuh.

4. **Biaya Operasi dan Latihan:** Mencakup biaya utilitas (listrik untuk pusat data sangat besar), biaya komunikasi satelit dan serat optik, serta pendanaan untuk pelaksanaan latihan internal, gabungan, maupun internasional.

Analisis tren belanja militer global oleh lembaga seperti SIPRI [47] menunjukkan bahwa negara-negara maju mengalokasikan porsi yang semakin besar dari anggaran pertahanan mereka untuk kapabilitas siber dan intelijen. Sebagai acuan, ASI perlu menargetkan alokasi bertahap hingga mencapai **1-2% dari total anggaran pertahanan nasional** saat beroperasi penuh.

8.2 Model dan Sumber Pembiayaan

Mengingat pentingnya misi dan sensitivitas operasinya, model pembiayaan ASI harus memprioritaskan keamanan dan kedaulatan.

1. **Sumber Utama: Anggaran Pendapatan dan Belanja Negara (APBN)** Pertahanan nasional adalah fungsi inti negara yang tidak dapat dikompromikan. Oleh karena itu, sumber pendanaan utama dan terbesar untuk ASI **harus berasal dari APBN murni** melalui alokasi di sektor pertahanan. Ketergantungan

pada APBN menjamin stabilitas pendanaan jangka panjang, independensi operasional, dan kerahasiaan yang mutlak, bebas dari pengaruh kepentingan komersial atau asing.

2. **Sumber Pelengkap: Kerja Sama Pemerintah dengan Badan Usaha (KPBU) / *Public-Private Partnership* (PPP)** Skema KPBU dapat dieksplorasi, namun **dengan batasan yang sangat ketat**. KPBU hanya dapat digunakan untuk mendanai infrastruktur pendukung yang bersifat **non-sensitif dan tidak terkait langsung dengan operasi tempur**. Contoh proyek yang bisa menggunakan skema KPBU [48] antara lain:

- Pembangunan gedung perkantoran umum atau asrama prajurit.
- Pengembangan platform e-learning untuk pelatihan dasar siber yang tidak rahasia.
- Proyek riset bersama dengan universitas atau BUMN pada teknologi *dual-use* (guna ganda).

3. **Secara tegas, kapabilitas inti seperti pusat data operasional, *Cyber Range*, platform intelijen, serta pengembangan dan akuisisi "senjata" siber tidak boleh dibiayai atau melibatkan pihak swasta, terutama asing.**

4. **Opsi Masa Depan: Dana Abadi Pertahanan Siber** Untuk menjamin keberlangsungan inovasi yang tidak terganggu oleh siklus anggaran tahunan, pemerintah dapat mempertimbangkan pembentukan **Dana Abadi Pertahanan Siber**. Dana ini dapat diisi dari alokasi awal APBN dan potensi kontribusi dari BUMN di sektor strategis. Hasil investasi dari dana abadi ini dapat digunakan secara khusus untuk membiayai riset dan pengembangan jangka panjang, memastikan ASI selalu berada di garis depan teknologi.

BAB 9: ROADMAP DAN IMPLEMENTASI

Pembentukan sebuah kekuatan militer baru adalah sebuah maraton, bukan lari cepat. Proses ini memerlukan perencanaan yang matang, komitmen politik yang kuat, dan eksekusi yang disiplin. *Roadmap* berikut dirancang sebagai panduan implementasi Angkatan Siber Indonesia (ASI) dalam tiga tahap utama, dengan kerangka waktu yang realistis dan target yang terukur. *Roadmap* ini bersifat dinamis dan dapat disesuaikan berdasarkan hasil evaluasi di setiap akhir tahapan.

9.1 Tahap I: Persiapan dan Peletakan Fondasi (2025 – 2026)

Fokus Utama: Membangun landasan hukum, doktrin, dan organisasi. Tahap ini lebih berfokus pada "perangkat lunak" (regulasi dan konsep) daripada "perangkat keras" (infrastruktur).

Target dan Aktivitas Kunci:

1. **Finalisasi Payung Hukum (Q1 2025 - Q4 2026):**

○ Membentuk tim kerja gabungan (Kemhan, Kemenkumham, Mabes TNI, Setneg) untuk menyusun naskah Peraturan Presiden (Perpres) tentang Pembentukan ASI sebagai Kotama Operasional TNI.

○ Melakukan advokasi dan konsultasi intensif dengan DPR RI dan lembaga terkait lainnya.

○ **Milestone:** Perpres ditandatangani oleh Presiden pada akhir tahun 2026.

2. **Pembentukan Tim Inti / Satuan Tugas (Q2 2025):**

○ Panglima TNI menunjuk sebuah tim inti (satuan tugas) yang dipimpin oleh seorang Perwira Tinggi (Pati) bintang satu atau dua sebagai manajer proyek pembentukan ASI.

- Tim ini akan menjadi cikal bakal staf pimpinan ASI dan bertanggung jawab mengawal seluruh aktivitas di Tahap I.

3. **Penyusunan Doktrin Fundamental (Q3 2025 - Q2 2026):**

- Tim inti menyusun draf awal dari dokumen-dokumen krusial, meliputi: Doktrin Operasi Siber TNI, Prosedur Tetap (Protap) Koordinasi dengan BSSN/BIN/Polri, dan kerangka Aturan Pelibatan (*Rules of Engagement*).

4. **Penilaian Kesiapan dan Perancangan Struktur (Q4 2025 - Q3 2026):**

- Melakukan *Security Readiness Maturity* (SRM) di seluruh lingkungan TNI untuk memetakan aset kritis dan kerentanan utama.

- Merancang struktur organisasi detail ASI hingga tingkat eselon terendah, lengkap dengan deskripsi tugas dan kualifikasi personel yang dibutuhkan.

- **Milestone:** Dokumen cetak biru organisasi dan kebutuhan personel selesai.

9.2 Tahap II: Pengembangan dan Pembangunan Kapasitas (2027 – 2029)

Fokus Utama: Pembangunan fisik, pengadaan teknologi, dan rekrutmen angkatan pertama. Tahap ini akan menjadi yang paling padat dalam hal belanja modal (CAPEX).

Target dan Aktivitas Kunci:

1. **Perekrutan dan Pelatihan Angkatan Pertama (Mulai Q1 2027):**

- Membuka pendaftaran rekrutmen perdana untuk perwira, bintara, dan tamtama ASI dari jalur karier militer dan sumber eksternal.

- Mengaktifkan Pusat Pembinaan Komponen Cadangan (Pusbin Komcad) Digital dan menyelenggarakan gelombang pertama pelatihan Komcad Digital.

2. **Pembangunan Infrastruktur Kritis (Mulai Q2 2027):**

- Memulai proses lelang dan konstruksi untuk Markas Besar ASI dan Pusat Data Nasional yang aman. Proyek ini bersifat multi-tahun.
- Membangun dan melengkapi fasilitas Pusdiklat Siber TNI dengan laboratorium dan *Cyber Range* generasi pertama.

3. **Aktivasi Unit Prioritas (Q1 2028 - Q4 2029):**

- Unit **Komando Pertahanan Siber (CDC)** dan **Batalyon Intelijen Digital (DIB)** menjadi yang pertama mencapai *Initial Operational Capability* (IOC).
- Fokus awal kedua unit ini adalah mengambil alih tugas pertahanan jaringan internal Mabes TNI dan Kementerian Pertahanan.
- **Milestone:** Jaringan pertahanan TNI secara resmi berada di bawah perlindungan aktif ASI pada akhir tahun 2029.

4. **Inisiasi Kemitraan Internasional (Sepanjang Tahap II):**

- Menandatangani nota kesepahaman (MoU) dengan angkatan siber negara-negara mitra.
- Mengirimkan gelombang pertama perwira untuk menempuh pendidikan dan pelatihan di luar negeri serta menerima instruktur asing untuk program *training-for-trainers*.

9.3 Tahap III: Operasional Penuh dan Modernisasi Berkelanjutan (2030 dan Seterusnya)

Fokus Utama: Mencapai kesiapan operasional penuh di seluruh spektrum dan memastikan keunggulan teknologi melalui inovasi berkelanjutan.

Target dan Aktivitas Kunci:

1. **Pencapaian *Full Operational Capability* (FOC) (Target Q4 2030):**

○ Seluruh lima unit fungsional (CDC, CAU, DIB, INO, dan Pusbin Komcad Digital) dinyatakan operasional penuh.

○ Markas Besar ASI dan Pusat Data telah beroperasi secara penuh.

○ ASI mulai melaksanakan seluruh misi yang diamanatkan dalam doktrinnya.

2. **Siklus Modernisasi Teknologi (Berkelanjutan):**

○ Menetapkan siklus pembaruan teknologi (misalnya setiap 3-5 tahun) untuk perangkat keras dan lunak inti guna mencegah keusangan teknologi.

○ Unit R&D internal secara aktif mengembangkan kapabilitas baru dan mempersiapkan transisi ke teknologi masa depan seperti *Post-Quantum Cryptography*.

3. **Evaluasi dan Pengembangan Doktrin (Setiap 2 Tahun):**

○ Melakukan evaluasi menyeluruh terhadap doktrin, taktik, teknik, dan prosedur (TTPs) berdasarkan pengalaman operasional, data intelijen ancaman terbaru, dan pelajaran dari konflik global.

4. **Kepemimpinan Regional (Target 2035):**

○ Bertransisi dari peserta menjadi penyelenggara atau tuan rumah bersama untuk latihan siber tingkat regional (ASEAN atau Indo-Pasifik), yang menandakan pengakuan atas kematangan dan kapabilitas ASI.

BAB 10: RISIKO DAN MITIGASI

Setiap inisiatif strategis berskala besar, terutama yang melibatkan pembentukan kekuatan militer dengan kapabilitas baru yang signifikan, pasti diiringi dengan serangkaian risiko. Perencanaan yang matang tidak hanya berfokus pada manfaat, tetapi juga secara proaktif mengidentifikasi potensi risiko dan merancang strategi mitigasi yang kuat sejak awal. Bab ini membahas risiko-risiko utama dalam pembentukan Angkatan Siber Indonesia (ASI) dan cara untuk mengelolanya.

10.1 Risiko Tumpang Tindih Wewenang dan Friksi Antar Lembaga

- **Risiko:** Pembentukan ASI berpotensi menciptakan persaingan atau kebingungan yurisdiksi dengan lembaga yang sudah ada seperti BSSN, BIN, dan Polri. Alih-alih sinergi, yang terjadi justru adalah perebutan wewenang (*turf wars*) yang dapat melumpuhkan respons negara saat menghadapi krisis siber.

- **Strategi Mitigasi:**

1. **Kerangka Hukum yang Definitif:** Instrumen hukum pembentukan ASI (Perpres atau UU) harus secara eksplisit mendefinisikan yurisdiksi, peran, dan yang terpenting, **mekanisme dan pemicu eskalasi**. Harus diatur dengan jelas bahwa mandat ASI berfokus pada ancaman dari aktor negara asing dan ancaman siber bereskalasi militer, yang dimulai saat mandat lembaga sipil berakhir.

2. **Formalisasi Forum Koordinasi:** Mengoperasionalkan **Forum Koordinasi Keamanan Siber Nasional** yang dipimpin oleh Menko Polhukam (seperti diusulkan di Bab 5) sebagai wadah permanen untuk dekonfliksi, berbagi informasi, dan pengambilan keputusan di tingkat strategis.

3. **Prosedur Tetap (Protap) dan Latihan Gabungan:** Mengembangkan dan mensosialisasikan Protap serah terima penanganan insiden antar lembaga. Latihan gabungan yang melibatkan skenario hibrida (melibatkan unsur kriminal, keamanan sipil, dan militer) harus digelar secara rutin untuk menguji dan memperkuat interoperabilitas serta membangun rasa saling percaya di tingkat operator.

10.2 Risiko Penyalahgunaan Kekuasaan dan Operasi Informasi

- **Risiko:** Kapabilitas siber ofensif dan operasi informasi ASI yang kuat dapat disalahgunakan untuk tujuan politik domestik, seperti mengawasi lawan politik, membungkam suara-suara kritis, atau menyebarkan propaganda untuk kepentingan penguasa. Ini adalah risiko paling sensitif yang dapat mendelegitimasi ASI.

- **Strategi Mitigasi:**

1. **Pembatasan Mandat yang Sangat Ketat:** Undang-undang harus secara tegas menyatakan bahwa target operasi ASI adalah **entitas asing dan ancaman eksternal**. Setiap operasi yang berpotensi menyasar target di dalam negeri harus melalui mekanisme otorisasi berlapis yang luar biasa ketat, idealnya hingga tingkat persetujuan Presiden dan disertai pertimbangan hukum yang kuat.

2. **Pengawasan Eksternal yang Independen:** Membentuk sebuah **Dewan Pengawas Independen** yang melapor langsung kepada Presiden dan DPR. Dewan ini dapat terdiri dari perwakilan Komisi I DPR, unsur Mahkamah Agung (hakim purnabakti), akademisi, dan tokoh masyarakat sipil yang kredibel. Dewan ini diberi wewenang untuk melakukan audit *post-facto* (setelah operasi selesai) terhadap operasi-operasi sensitif ASI.

10.3 Risiko Pelanggaran Privasi Warga Negara

- **Risiko:** Dalam menjalankan fungsi intelijen sinyal (SIGINT), ASI dapat melakukan pengawasan massal (*bulk surveillance*) yang tidak terarah dan melanggar hak privasi warga negara Indonesia yang dijamin oleh Konstitusi dan UU Pelindungan Data Pribadi (UU PDP).

- **Strategi Mitigasi:**

1. **Prinsip Penargetan dan Minimalisasi Data:** Operasi intelijen ASI harus didasarkan pada prinsip **penargetan yang spesifik** terhadap entitas asing yang dicurigai, bukan pengumpulan data massal tanpa pandang bulu.

2. **Implementasi Teknologi Pelindung Privasi:** Mengadopsi teknologi dan prosedur yang secara otomatis mampu menganonimkan atau membuang data warga negara Indonesia yang secara tidak sengaja ikut terambil dalam sebuah operasi intelijen yang sah.

3. **Mekanisme Otorisasi Yudisial:** Untuk operasi intelijen siber di dalam negeri yang berisiko tinggi menyentuh data warga negara, pelaksanaannya harus didahului oleh surat perintah atau izin dari pengadilan yang ditunjuk secara khusus, serupa dengan praktik di negara-negara demokrasi lainnya.

10.4 Risiko Ketergantungan pada Teknologi Asing

- **Risiko:** Demi mengejar pembangunan yang cepat, ASI menjadi terlalu bergantung pada perangkat keras, perangkat lunak, dan data intelijen dari satu negara atau blok tertentu. Ketergantungan ini menciptakan kerentanan strategis: teknologi tersebut bisa saja memiliki *backdoor*, atau aksesnya dapat diputus sebagai alat tawar politik saat terjadi krisis diplomatik.

- **Strategi Mitigasi:**

1. **Kebijakan Akuisisi Multi-Vendor:** Menerapkan kebijakan pengadaan yang melarang ketergantungan pada satu vendor tunggal untuk sistem yang kritikal. Diversifikasi sumber teknologi dari berbagai negara yang berbeda.

2. **Mendorong Industri Pertahanan Siber Dalam Negeri:** Menjalankan secara konsisten peta jalan kemandirian teknologi (seperti di Bab 7) dengan memberikan insentif, pendanaan riset, dan kontrak jangka panjang kepada BUMNIS, BRIN, universitas, dan perusahaan swasta nasional untuk mengembangkan produk keamanan siber sendiri.

3. **Uji Tuntas Keamanan yang Ketat:** Semua teknologi impor, sebelum dipasang di jaringan sensitif, wajib melalui proses audit keamanan dan analisis kode sumber yang mendalam oleh tim independen di bawah Kemhan atau BSSN.

BAB 11: TATA KELOLA DAN EVALUASI

Untuk memastikan Angkatan Siber Indonesia (ASI) senantiasa akuntabel, efektif, dan relevan dengan perkembangan zaman, diperlukan sebuah kerangka tata kelola dan evaluasi yang kokoh. Mekanisme ini bertujuan untuk mengukur kinerja, memastikan kepatuhan terhadap hukum, dan menjadi dasar bagi perbaikan berkelanjutan.

11.1 Model Pemeriksaan Periodik

ASI akan dievaluasi secara komprehensif dan periodik, dengan siklus **setiap dua tahun sekali**. Evaluasi ini dilakukan oleh **Tim Audit Gabungan** yang bersifat independen dan terdiri dari beberapa unsur:

1. **Badan Pemeriksa Keuangan (BPK):** Melakukan audit keuangan secara menyeluruh untuk memastikan pengelolaan anggaran ASI transparan, efisien, dan akuntabel sesuai peraturan yang berlaku.

2. **Komisi I Dewan Perwakilan Rakyat (DPR RI):** Menjalankan fungsi pengawasan politik terhadap keselarasan kebijakan dan operasi ASI dengan arah kebijakan pertahanan negara, serta efektivitasnya dalam mencapai tujuan nasional.

3. **Dewan Pengawas Independen:** Sebagaimana diusulkan pada Bab 10, dewan ini akan melakukan audit kepatuhan (*compliance audit*) terhadap pelaksanaan operasi-operasi sensitif, memastikan ASI tetap berada dalam koridor hukum, menghormati hak asasi manusia, dan tidak menyalahgunakan wewenangnya.

Hasil dari audit gabungan ini akan dilaporkan langsung kepada Presiden dan DPR sebagai bahan pertimbangan untuk kebijakan di masa mendatang.

11.2 Indikator Capaian Kinerja (KPI)

Evaluasi kinerja ASI tidak bersifat subjektif, melainkan diukur melalui serangkaian Indikator Capaian Kinerja (*Key Performance Indicators* - KPI) yang kuantitatif dan kualitatif. KPI utama meliputi:

- **Kesiapan Operasional:**

  - **Waktu Respons Insiden:** Pengukuran *Mean Time to Detect* (MTTD) dan *Mean Time to Respond* (MTTR) terhadap ancaman siber di jaringan pertahanan. Targetnya adalah menurunkan angka ini secara konsisten dari tahun ke tahun.

  - **Tingkat Netralisasi Ancaman:** Jumlah serangan siber tingkat tinggi (*Advanced Persistent Threats*) yang berhasil dideteksi, ditahan, dan dinetralisir sebelum menyebabkan kerusakan signifikan.

- **Pengembangan SDM:**

  - **Jumlah Personel Tersertifikasi:** Persentase personel operasional yang memegang sertifikasi keamanan siber profesional yang diakui secara internasional (misalnya OSCP, CISSP, GCIH).

  - **Tingkat Retensi Personel Ahli:** Kemampuan ASI untuk mempertahankan para talenta terbaiknya setelah masa ikatan dinas pertama selesai, yang mengindikasikan kepuasan dan jalur karier yang baik.

- **Kematangan Proses dan Teknologi:**

  - **Skor *Maturity Level*:** Penilaian tingkat kematangan proses dan kapabilitas ASI secara berkala menggunakan kerangka kerja standar internasional seperti **NIST Cybersecurity Framework (CSF)** [28] dan **Capability Maturity Model Integration (CMMI)** [29]. Targetnya adalah mencapai tingkat "Managed" atau "Optimizing" dalam 10 tahun pertama operasi.

BAB 12: STUDI PERBANDINGAN INTERNASIONAL

Usulan pembentukan ASI bukanlah sebuah loncatan ke dalam ketidaktahuan. Konsep ini dibangun di atas pelajaran dan praktik terbaik (*best practices*) dari berbagai negara yang telah lebih dulu menavigasi kompleksitas pertahanan di ranah maya.

- **Amerika Serikat (USCYBERCOM & CISA):** Pelajaran utama adalah pentingnya **pembagian peran yang jelas antara militer dan sipil**. USCYBERCOM [29] fokus pada spektrum operasi militer, sementara CISA [49] memimpin perlindungan infrastruktur kritis federal dan sipil. Model ini menjadi acuan ideal bagi hubungan sinergis antara ASI dan BSSN.

- **Singapura (Digital and Intelligence Service - DIS):** Singapura mengajarkan pentingnya **pendekatan holistik terhadap domain informasi**. Dengan menyatukan fungsi siber, intelijen, dan operasi pengaruh (*influence operations*) dalam satu matra (DIS) [30], Singapura mengakui bahwa perang modern dimenangkan dengan menguasai keseluruhan ekosistem informasi, bukan hanya aspek teknisnya.

- **Estonia (Cyber Defence League):** Pengalaman Estonia pasca-serangan siber besar-besaran tahun 2007 melahirkan *Cyber Defence League* [50], sebuah milisi siber sukarela. Ini adalah bukti nyata efektivitas konsep **pertahanan semesta**, di mana talenta sipil terbaik dapat dimobilisasi secara cepat dan terorganisir, menjadi justifikasi kuat bagi konsep Komponen Cadangan (Komcad) Digital di Indonesia.

- **Australia (Australian Signals Directorate - ASD):** Model ASD [51] menunjukkan efisiensi dari penggabungan tiga fungsi kunci—**intelijen sinyal asing, pertahanan siber, dan operasi siber ofensif**—di bawah satu lembaga yang memiliki sejarah panjang dalam dunia intelijen.

- **NATO CCDCOE & IMPACT:** Dari aliansi dan organisasi internasional, pelajaran utamanya adalah **keniscayaan kerja sama internasional**. Ancaman siber tidak mengenal batas negara. Latihan bersama seperti *Locked Shields* [52] dan platform berbagi informasi seperti yang diprakarsai oleh ITU [18] adalah elemen vital untuk membangun pertahanan kolektif dan saling percaya.

BAB 13: REFERENSI (DAFTAR PUSTAKA)

Berikut adalah daftar sumber daya yang menjadi acuan dalam penyusunan *whitepaper* ini.

Regulasi & Dokumen Resmi (12)

1. Undang-Undang No. 3 Tahun 2002 tentang Pertahanan Negara.
2. Undang-Undang No. 34 Tahun 2004 tentang Tentara Nasional Indonesia.
3. Undang-Undang No. 19 Tahun 2016 tentang Perubahan atas UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
4. Undang-Undang No. 23 Tahun 2019 tentang Pengelolaan Sumber Daya Nasional untuk Pertahanan Negara.
5. Undang-Undang No. 27 Tahun 2022 tentang Pelindungan Data Pribadi.
6. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.
7. Peraturan Presiden No. 47 Tahun 2023 tentang Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
8. Peraturan Badan Siber dan Sandi Negara No. 1 Tahun 2024 tentang Tata Kelola Strategi Keamanan Siber Nasional dan Manajemen Krisis Siber.
9. Peraturan Badan Siber dan Sandi Negara No. 2 Tahun 2024 tentang Tim Tanggap Insiden Siber.
10. Laporan Tahunan Lanskap Keamanan Siber Indonesia. Badan Siber dan Sandi Negara (BSSN).

11. US Cyber Command. (2018). *Doctrine for the Cyberspace Domain: Cyberspace Operations*.
12. Singapore Armed Forces. (2022). *Fact Sheet: The Digital and Intelligence Service (DIS)*.

Jurnal Ilmiah & Akademik (15)

13. Jurnal Pertahanan & Bela Negara. "Konseptualisasi Perang Siber dalam Doktrin Pertahanan Indonesia."
14. Jurnal Studi Pemerintahan, Universitas Padjadjaran. "Analisis Tumpang Tindih Kewenangan Lembaga Siber di Indonesia."
15. Jurnal Hukum Internasional, Universitas Indonesia. "Applicability of International Humanitarian Law in Cyberspace."
16. Arifin, T. (2021). "Urgensi Pembentukan Komando Pertahanan Siber (Kohanber) TNI." *Jurnal Strategi Pertahanan Semesta*.
17. Schmitt, M. N. (Ed.). (2017). *The Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.
18. Healey, J. (2019). "The Implications of Militarizing Cyberspace." *Journal of Cybersecurity*.
19. Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.
20. Slay, J., & Simon, M. (2007). "The role of the expert witness in computer forensics cases." *Journal of Digital Investigation*.
21. Manoppo, V. (2022). "Cyber Diplomacy in Indonesia's Foreign Policy." *Jurnal Hubungan Internasional*.
22. Laporan Penelitian CSIS Indonesia. "Tantangan dan Arah Kebijakan Keamanan Siber Indonesia."
23. Maksum, I. (2023). "Public-Private Partnership in Indonesian Defense Industry." *Indonesian Journal of Defense & Security*.
24. Belfer Center for Science and International Affairs, Harvard Kennedy School. (2020). "Models of National Cyber Command."
25. European Union Agency for Cybersecurity (ENISA). "National Cybersecurity Strategies - Best Practices."
26. Jurnal Universitas Pertahanan. "Pengembangan Sumber Daya Manusia Unggul untuk Menghadapi Ancaman Siber."
27. Nugroho, Y. (2021). "Civil-Military Relations in Indonesia's Cybersecurity Governance." *Asian Journal of Political Science*.

White Paper & Laporan Industri Internasional (10)

28. NIST. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (NIST CSF) Version 1.1*.
29. CMMI Institute. (2021). *Cybersecurity Maturity Model Certification (CMMC)*.
30. Mandiant (a Google Cloud company). (2024). *M-Trends 2024 Report*.
31. Council on Foreign Relations. (2022). *Confronting Reality in Cyberspace: Foreign Policy for a Fragmented Internet*.
32. RAND Corporation. (2020). *Building a Stronger Cyber Force: A Review of an Army Cyber-Branch Proposal*.
33. International Institute for Strategic Studies (IISS). (2021). *Cyber Capabilities and National Power: A Net Assessment*.
34. (ISC)². (2023). *Cybersecurity Workforce Study*.
35. Gartner. (2024). *Top Trends in Cybersecurity 2024*.
36. World Economic Forum. (2024). *Global Cybersecurity Outlook 2024*.
37. SIPRI. (2024). *Trends in World Military Expenditure, 2023*.

Berita & Laporan Media (10)

38. Antara News. "TNI Gelar Latihan Gabungan Pertahanan Siber untuk Hadapi Ancaman Modern."
39. Kompas.id. "Analisis Kebocoran Data KPU dan Implikasinya pada Kepercayaan Publik."
40. The Diplomat. "Indonesia's Cybersecurity Cooperation with Australia and the US."
41. Modern Diplomacy. "Indonesia's Cyber Defense Posture in the Indo-Pacific."
42. Hukumonline. "Menelaah Arah Kebijakan Strategi Keamanan Siber Nasional dalam Perpres 47/2023."
43. SSEK Indonesian Legal Consultants. "The Indonesian Personal Data Protection Law: A New Era for Data Governance."
44. Reuters. "Ukraine's 'IT Army' of Counter-Hackers: How It Works."
45. Channel News Asia. "Inside Singapore's New Digital and Intelligence Service."
46. BBC News. "Estonia: The Digital Republic and its Cyber Defences."
47. The Jakarta Post. "Indonesia's Pressing Need to Establish a Cyber Force."

Situs Resmi & Lainnya (5)

48. Situs Resmi Badan Siber dan Sandi Negara (BSSN): bssn.go.id
49. Situs Resmi Kementerian Pertahanan Republik Indonesia: kemhan.go.id

50. Situs Resmi NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE): ccdcoe.org
51. Situs Resmi U.S. Cybersecurity and Infrastructure Security Agency (CISA): cisa.gov
52. Situs Resmi Australian Signals Directorate (ASD): asd.gov.au

---

KESIMPULAN

Dunia telah berubah. Medan pertempuran masa depan tidak lagi terbatas di darat, laut, dan udara. Kedaulatan sebuah bangsa kini turut dipertaruhkan di ranah maya. Menghadapi realitas ancaman siber yang semakin canggih, persisten, dan disponsori oleh negara, Indonesia tidak bisa lagi bertahan dengan postur yang terfragmentasi dan reaktif. Diperlukan sebuah lompatan strategis untuk menjamin keamanan dan kepentingan nasional di abad ke-21.

Angkatan Siber Indonesia (ASI) adalah jawaban atas tantangan tersebut. Sebagai komando utama operasional di bawah Panglima TNI, ASI akan menjadi kekuatan militer siber yang profesional, terpadu, dan modern. Pembentukannya akan **mengkonsolidasikan kekuatan** siber yang tersebar, **memperjelas rantai komando** dalam situasi krisis, serta memberikan **efek gentar** yang kredibel terhadap siapapun yang berniat jahat terhadap kedaulatan digital Indonesia.

Dengan landasan hukum yang kokoh, SDM yang unggul, teknologi yang mumpuni, serta tata kelola yang akuntabel, ASI bukan hanya akan menjadi perisai, tetapi juga tombak yang akan menjamin Indonesia tidak hanya selamat, tetapi juga berdaulat dan berjaya di era digital. Ini adalah sebuah investasi untuk masa depan, sebuah keniscayaan untuk menjaga keutuhan Negara Kesatuan Republik Indonesia.

LANGKAH SELANJUTNYA

Untuk menerjemahkan proposal dalam *whitepaper* ini menjadi kenyataan, diperlukan langkah-langkah konkret dan segera sebagai berikut:

1. **Validasi dan Konsultasi Awal:** Mempresentasikan dokumen ini secara resmi kepada para pemangku kepentingan kunci, termasuk pimpinan Kementerian Pertahanan, Mabes TNI, BSSN, BIN, Kominfo, dan Komisi I DPR RI untuk mendapatkan masukan awal dan membangun pemahaman bersama.

2. **Pembentukan Tim Kerja Antar-Kementerian:** Mendorong pembentukan tim kerja atau satuan tugas resmi yang diberi mandat untuk mengkaji secara mendalam proposal ini dan mulai menyusun draf awal instrumen hukum yang diperlukan (Peraturan Presiden).

3. **Advokasi Politik dan Legislasi:** Setelah draf matang, melakukan advokasi politik kepada pimpinan nasional untuk mendapatkan dukungan penuh, sehingga proses penetapan payung hukum pembentukan Angkatan Siber Indonesia dapat segera dimulai.